International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 9936-9941
© Research India Publications. http://www.ripublication.com

A Study on Improvement of Personal Information Divulgence Prevention System (A case of the Health and Welfare Division)

Ya-Ri Lee[*], Jung-Sook Kim[**], Ho-Kyun Park[***]
** Somansa Consulting Center Co., Ltd.*
Seoul 07228, Republic of Korea.
*** Division of Computer Engineering & Mechatronics, Sahmyook University*
Seoul 01795, Republic of Korea.
**** School of IT Convergence Engineering, Shinhan University*
Gyeonggi-do 11340, Republic of Korea.

**Corresponding author: Jung-Sook Kim, Ph.D.*

Abstract

Recently, there has been a growing public concern over the mass leak of personal information. The health and welfare division, which handles sensitive information such as health and diseases, is the primary target of cyber attacks such as hacking, although it is essential to operate a homepage for public and private companies. This is a strategy to improve the homepage personal information divulgence prevention monitoring system after the information and homepage addresses of the target organizations are made current through case analysis of current monitoring system operated for personal information divulgence prevention in health and welfare division homepages. This is a DB check method that uses the best personal information as the priority of search information, and we proposed a quantitative and qualitative improvement plan through wide diagnosis and archive analysis for the establishment of quick response system of personal information leakage accident.

Keywords: Divulgence Prevention, Monitoring, Validation check, Wide diagnostic, Archive analysis

INTRODUCTION

Preemptive response and integrated control for divulgence prevention of personal information is an indispensable task in the homepage where the public service is performed. In the main homepage of the health and welfare division, which is one of the representative services of the general public, an on-going monitoring system has been introduced and operated from 2012 to build rapid response system for personal information leakage [1][2]. The current system confirms the changes in the homepage list of the Ministry of Health and Welfare and the affiliated institutions' homepage, which is estimated to be between 400 and 500, twice a year, and is being actualized in the monitoring system. In addition, divulgence prevention monitoring and diagnosis of homepage personal information are performed twice a month, and personal identification information, which is personal information exposed to major portals once a month, is monitored [3]. Figure 1 is a conceptual diagram of the current system. It consists of exposure monitoring solution and operation management system for personal information, and performs main functions such as exposure check and history management of personal information of web pages per domain [4].

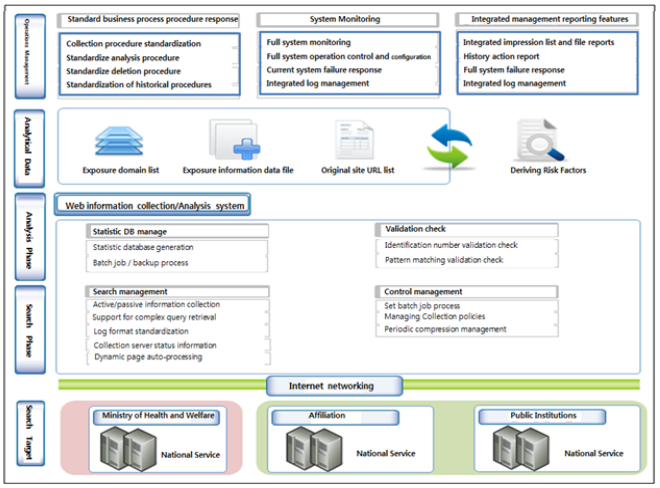

Figure 1. Personal Information Divulgence Prevention Monitoring System Configuration

The divulgence prevention monitoring procedure for personal information in the homepage of the health and welfare division consists of five stages as shown in Figure 2. After personal information is collected, it is detected and analyzed, and the process of exposure response is followed. And it is operated in a way that integrates and manages collected and analyzed information [3].

Figure 2. Personal Information Divulgence Prevention Monitoring Process

RELATED WORKS

Privacy Level Management

Personal information can trigger additional damage such as invasion of privacy, financial damage, and illegal use of others' names, and so people's anxiety is continuously growing. Also, it is emerging to a major threat to institutions and firms as to image destruction, consumer confidence losses, revenue decrease, class action, and damage compensation [5].

Ministry of Government Administration and Home Affairs plans inspects personal information protection status, analyzes information system vulnerability and improves at government level as illustrated in Figure 3[6][7][8][17].

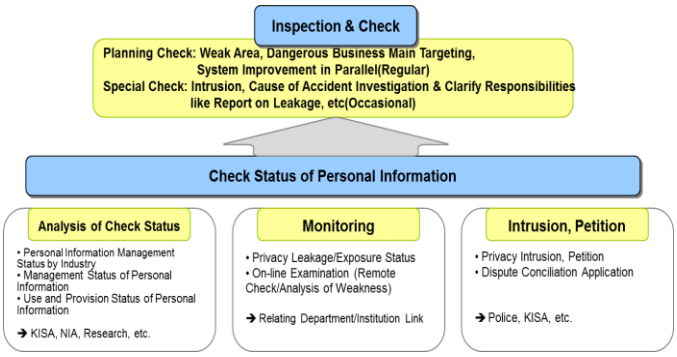

Figure 3. Ministry of Government Administration and Home Affairs personal information protection status inspection.

Problems of personal information disclosure

Exposure of personal information through the homepage refers to the state where related information is left on the Internet so that the user of the homepage can acquire the personal information of the other person while using the Internet without using special methods such as hacking. This condition is caused by negligence or carelessness. However, information that may be infringing privacy, such as personal identification information, credit card number, account number, and bio information, should never be exposed. And unique identification information refers to resident registration number, passport number, driver's license number, and alien registration number. Particularly in the related laws such as the Personal Information Protection Law of Korea, the resident registration number is important information that cannot be processed without the legal grounds even if the consent of the person is present, and the passport number is important information that the consent of the person is required and encrypted. If we look at the sanctions related to the disclosure of personal information in Korea, we will carry out the technical, administrative and physical measures necessary to ensure safety such that personal information or unique identification information, which is a "safety obligation", should not be lost, stolen, leaked, altered, Article 24 (4) and Article 29 ". The Ministry of Government Administration and Home Affairs has prescribed and notified the details necessary for the Act, and the main contents are to make measures for access control such that personal information is not disclosed or leaked to the person who does not have the right to browse through the internet homepage and the open wireless network And check the vulnerability at least once a year so that unique identification information is not leaked, altered, or damaged through the Internet homepage. If we fail to fulfill these obligations, you will be charged a fine of up to KRW 30 million. If you do not, you may be punished by imprisonment for up to two years or a fine of up to KRW 10 million.

Another problem with personal information exposure on the homepage is the secondary exposure to search engines such as Google. If the personal information exposed on the homepage is not promptly deleted, the exposure may spread by the search engine such as Google, or it may be collected by a third party. Therefore, an individual may be abused for crime such as impersonation, voice phishing, we may be injured. Information that is exposed in this way is collected and analyzed as an individual. It may be exploited as a violation of privacy, and companies may be subject to image distortion and damages caused by multiple victims [9-15][18].

DISCUSSION

For divulgence prevention of personal information in homepage, it is essential to update the information with accurate information to maintain the latest information in the process of regularly or irregularly updating the address information of the monitoring target website. Therefore, it is always checked whether the homepage is changed so that divulgence prevention monitoring can be performed and that information is not omitted even in case of change of the person in charge of the target organization, homepage change, and new establishment.

Improvements to the address list actualization procedure

Periodical actualization of target list for the homepage personal information divulgence prevention monitoring is conducted through three steps of actualization request, data collection and review, and system application as shown in Figure 4. First, the homepage list information of the monitoring target is requested to the person in charge of the target homepage. In the next step, the target list of the

collected institutions is collected, the validity of the homepage is examined, and errors and changes are identified. At the final stage, after a detailed review of the change information, the checking process of the monitoring system is modified and applied, and a test for operation is performed [16].

In the current system, since the homepage system of the target institution is added and upgraded, the updated list is ineffective because it includes the task of manually updating the updated homepage information in the target institution as shown in Figure 5.

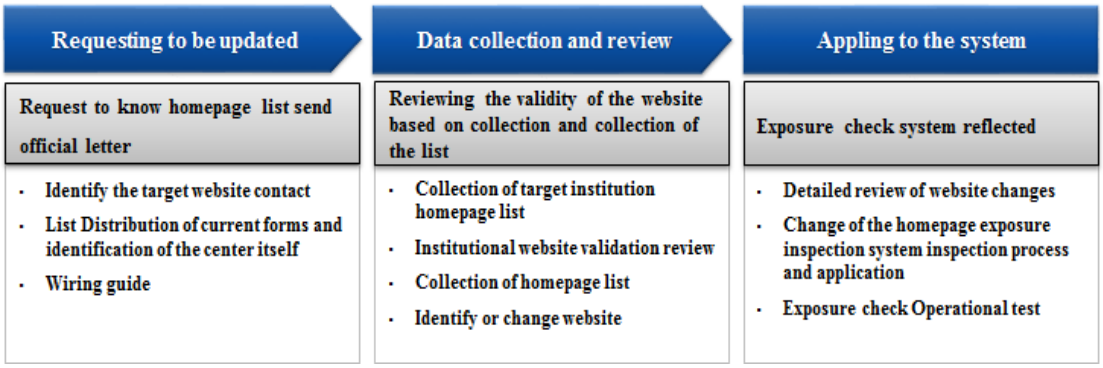

Figure 4. Procedures to regularly update the list of monitored objects

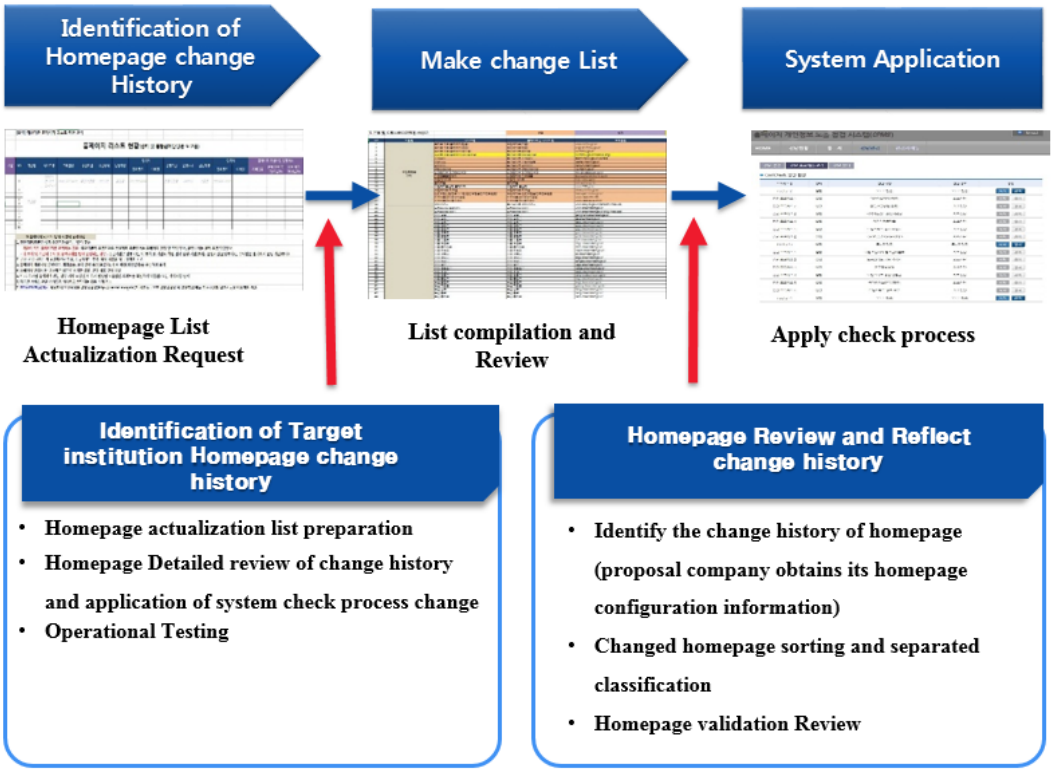

Figure 5. Procedures for updating the changed homepage

To solve these problems, this study proposed a wide diagnosis and archive analysis diagnostic method by adding a selective classification system and a validity review module for modified homepage information. Wide diagnosis is a method of expanding the homepage range of the homepage divulgence prevention monitoring system as shown in Figure 6, and further diagnosing the homepage belonging to the check target domain for accurate diagnosis.

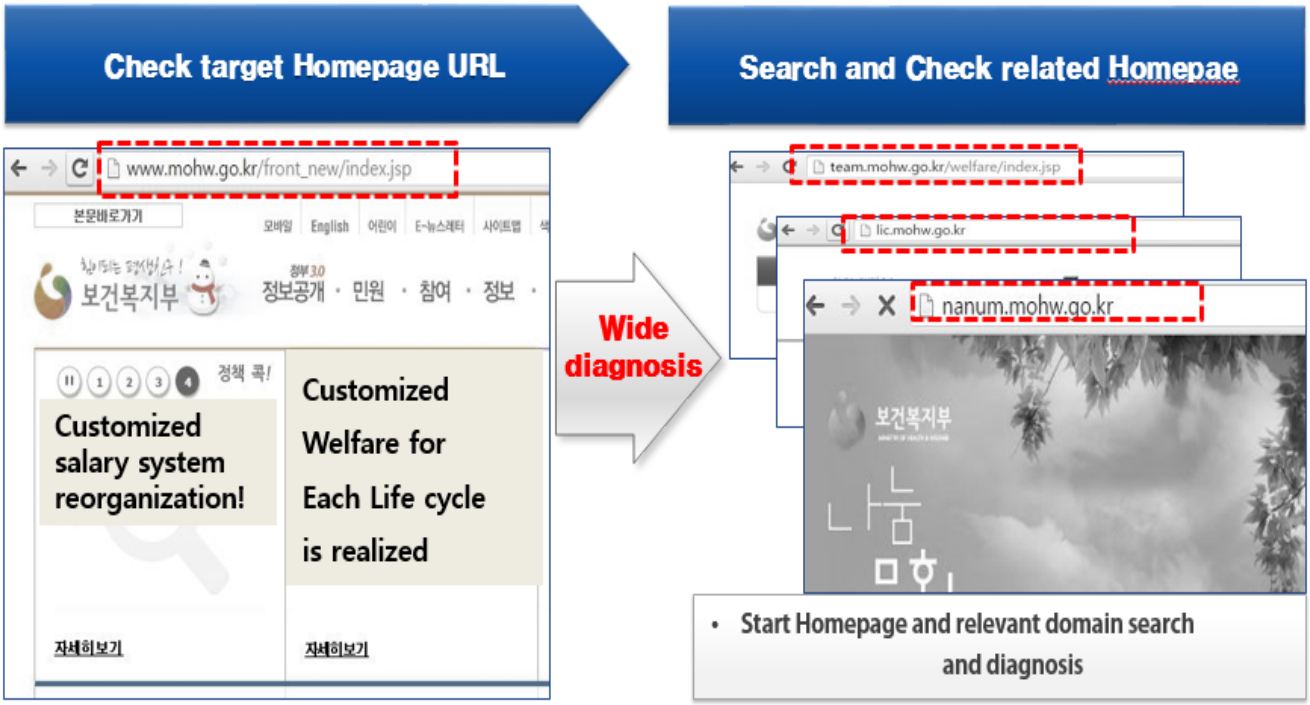

Figure 6. Search and check of related homepage through wide diagnosis

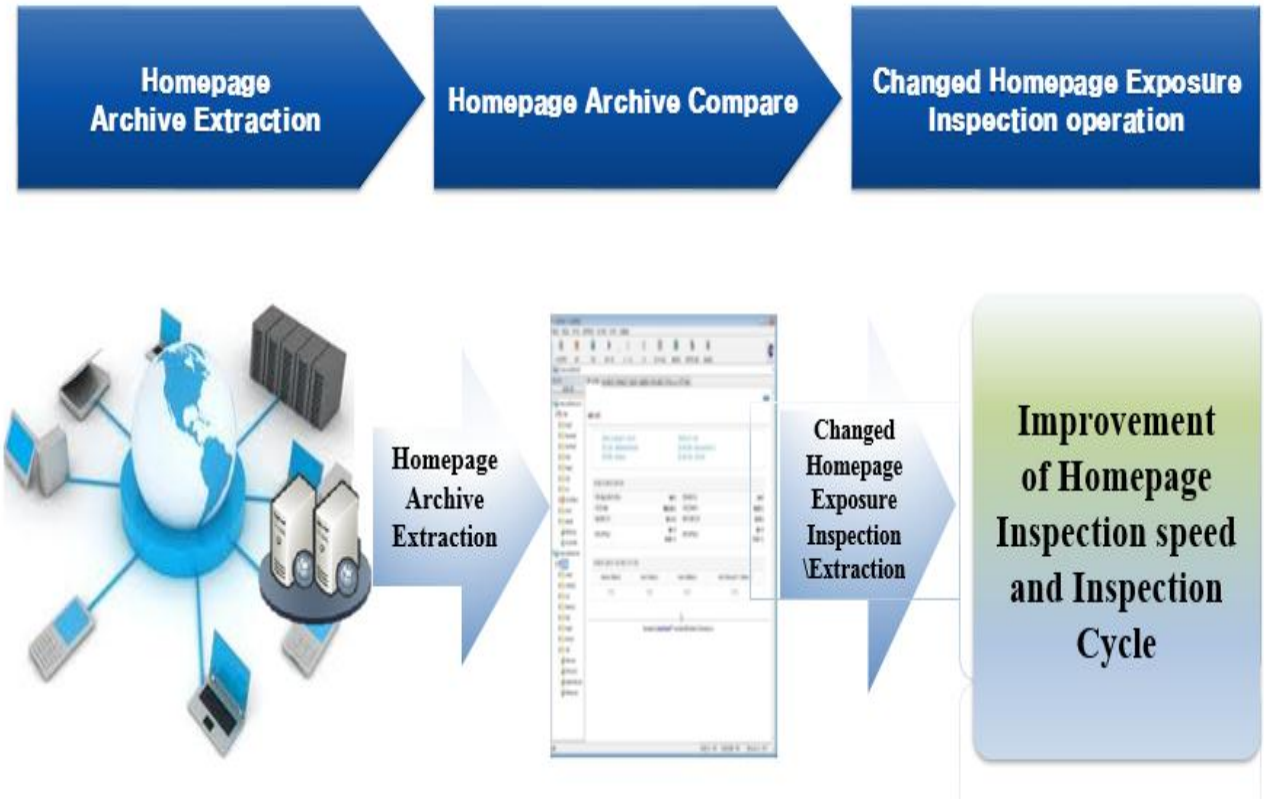

Figure 7. Checking the changed homepage through archive analysis

The diagnostic method for archive analysis is to find and identify the homepage with the change as shown in Figure 7.

Improvement of divulgence prevention monitoring system operation of personal information

The operation of personal information divulgence prevention monitoring system in Health and welfare division as shown in Figure 8, the target homepage is divided into the homepage for the main inspection and the website for the non-main monitoring [4].

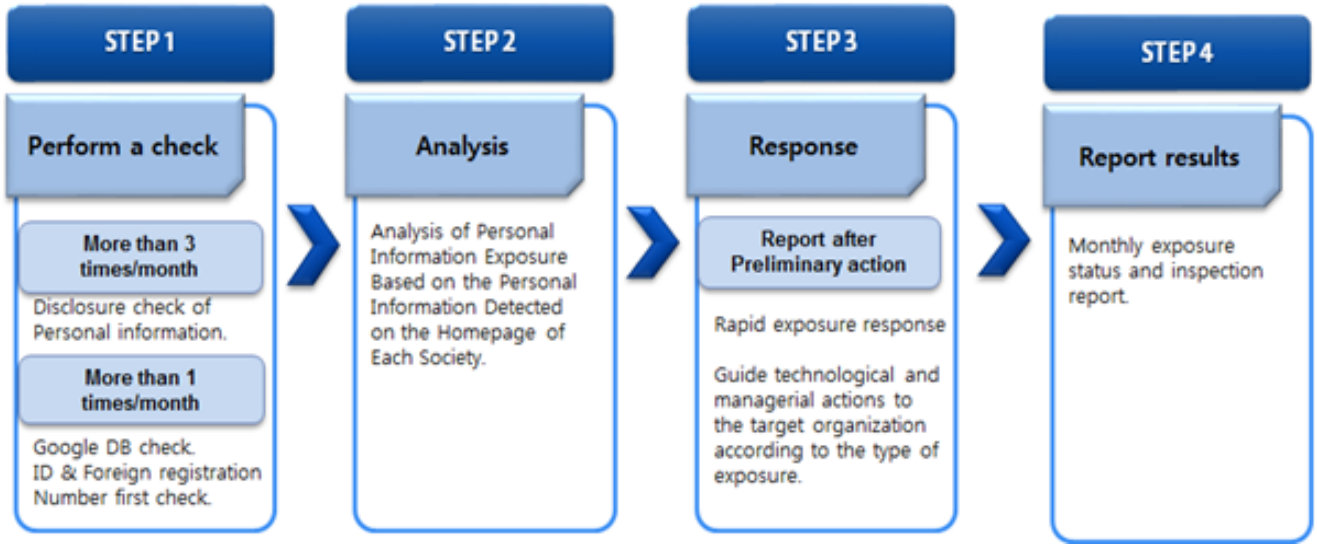

Figure 8. Personal Information Divulgence Prevention Monitoring Operating Process

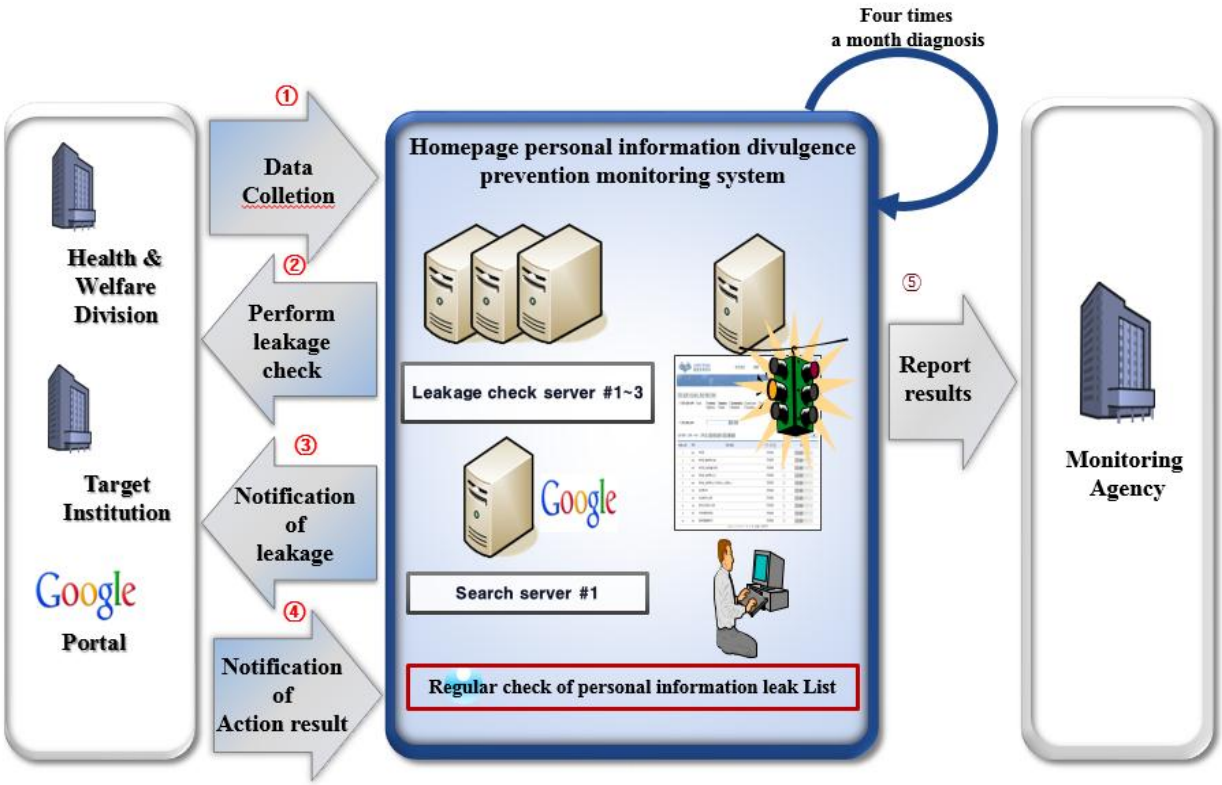

Figure 9. Improvement plan for personal information leakage prevention monitoring system on the homepage.

This method of operation checks only the expected homepage in advance, so that there is a problem that an unexpected problem in a web site cannot be detected early. Therefore, in this study, we propose a method as shown in Figure 9. This method increases the monitoring frequency of major web sites from current 3 times to 4 times per month and selects the resident registration number and alien registration number as the priority among the search information used in the Google DB check to determine the optimal personal information divulgence prevention, which is an improvement strategy for the operation in a manner of monitoring.

CONCLUSION

This study analyzed the case of divulgence prevention monitoring system of homepage personal information currently in service for the health and welfare division. This study suggested an improvement strategy of the divulgence prevention monitoring system of homepage personal information. Currently, the divulgence prevention monitoring system of personal information consists of five steps including management of target homepage information, check for leakage, response, post management, measures and improvement. In the first step of the present system, it is necessary is to add a method of upgrading to improve the effectiveness of the divulgence prevention monitoring when applying to the system through collecting and reviewing information (deletion, addition, change) of the homepage managed by the institution. Therefore, in this study, to expand the range of check homepage and for accurate diagnosis, we proposed quantitative and qualitative improvement as a diagnostic method through a wide diagnosis for the homepage belonging to the check domain and an archive analysis for finding the changed homepage.

REFERENCES

[1] Choi Jin-young, Ha Tae-gyun, Lee Kang Shin, Won Yu Jae, Privacy Incident Response System, Journal of The Korea Institute of Information Security & Cryptology Vol.19, No.6, Dec. (2009), pp.9-14.

[2] Privacy Guidelines, Ministry of Health and Welfare, (2016).

[3] Private Information Control Center Consignment Business, Ministry of Health and Welfare, (2014).

[4] Establish Personal Information Exposure Monitoring System and Improve Personal Information Integration Control System, Korea Institute for Health and Social Affairs, (2012).

[5] Chae-Yong Jung, Jin-Goo Choi, Kyeong-Seok Han, Yong-Lak Choi, An Empirical Study on Private Information Leakage Prevention Method in the Field of Health and Welfare, IT Policy Management, Vol. 5, No. 1, (2013), pp.134-140.

[6] The Effects of the Operation of an Information Security Management System on the Performance of Information Security, Journal of KIISE : Information Networking, Vol. 40, No. 1, (2013), pp.58-69.

[7] Ministry of Government Administration and Home Affairs, Public institution privacy management level diagnostic manual, (2014).

[8] Ministry of Government Administration and Home Affairs, Privacy self-diagnostic checklist, (2014).

[9] Young-Chul Chung, De-identification Policy of Personal Information and Tasks on Healthcare Big Data, Health and Welfare Forum, Vol. 227, (2015), pp50-60.

[10] Privacy Commission. A study on the effects of personal information de-identification on personal information protection, (2015).

[11] HHS OCR, Guidance Regarding Methods for De-identifacation of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act(HIPAA) Privacy Rule, (2012).

[12] National Information Society Agency, Casebook of personal information de-identification for the utilization of Big Data, Ministry of Science, ICT and Future Planning, (2014).

[13] Article 29 Data Protection Working Party(2014.04.), [Opinion 05/2014 on Anonymisation Techniques],

http://ec.europa.eu/justice/data-protection/index_en.htm

[14] Han Eun-Young, Japan's revised personal information protection laws, KISDI, (2015).

[15] U.K ICO: Managing data protection risk code of practice.

[16] Website Privacy Prevention Guidelines, Ministry of Government Administration and Home Affairs, (2014).

[17] Ya-Ri Lee, Kyong-Pyo Hong, Jung-Sook Kim, Ho-Kyun Park, A Study of Privacy Level Management System Establishment for Health and Welfare Sector, International Journal of Software Engineering and Its Applications Vol. 9, No. 11 (2015), pp. 237-246.

[18] Ya-Ri Lee, Young-Chul Chung, Jung-Sook Kim, Ho-Kyun Park, Personal Health Information De-identified Performing Methods in Big Data Environments, International Journal of Software Engineering and Its Applications, Vol. 10, No. 8 (2016), pp. 127-138.